



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/722,487 | 11/28/2003 | Tadashi Kojima | 246038US2S | 1194 |

22850 7590 04/12/2007
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

| |
|----------|
| EXAMINER |
|----------|

HOANG, DANIEL L

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2136

| SHORTENED STATUTORY PERIOD OF RESPONSE | NOTIFICATION DATE | DELIVERY MODE |
|--|-------------------|---------------|
| 3 MONTHS | 04/12/2007 | ELECTRONIC |

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/12/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary

Application No.

10/722,487

Applicant(s)

KOJIMA ET AL.

Examiner

Daniel L. Hoang

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 May 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 May 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date See Continuation Sheet.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :11/28/03, 6/03/05, 10/04/05, 11/08/05.

DETAILED ACTION

CLAIMS PRESENTED

Claims 1-20 are presented.

CLAIM REJECTIONS

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2, 4 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 2:

The claim recites the limitation, "each of which is encrypted separately" on line 4. It is unclear to examiner what "each of which" is intended to be applied to. As the claim currently stands, it could be interpreted that applicant intends to claim that each of the plurality of first keys are encrypted. It can also be interpreted that applicant intends to claim that each of the plurality of content data is encrypted. Or it may be interpreted that both pluralities of first keys and content data are encrypted. Further, the claim also recites the limitation "separately" on line 4. It is unclear to examiner whether this means that the first key and the content data are encrypted separately or whether it means each individual first key and/or content data are encrypted separately. As such, the claim is rendered vague and indefinite. For purposes of examination, examiner interprets that the claim is intended to mean that each first key and each content data are encrypted separately. Appropriate correction is required.

Art Unit: 2136

As per claim 4:

The claim recites the limitation "identical" on line 5. It is unclear to examiner what applicant intends to mean by claiming that both recording mediums are identical. It could be interpreted that both recording mediums are identical in size or type. Or they can be identical in that they both contain the same content. For purposes of examination, examiner is interpreting that the claim means to say that both recording mediums are identical in that they both have keys recorded therein.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-10, 13-15, and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishibashi et al., US PGP No. 20050005148, hereinafter reference 1, and further in view of Ishibashi et al., US PGP No. 20070030974, hereinafter reference 2.

As per claims 1, 14, 18:

Reference 1 teaches:

A content management method, comprising:

encrypting content data by a first key;

[see ¶0058] "contents data encrypted by contents key Kc"

encrypting the first key by predetermined plural types of second keys;

[see ¶0058] "contents key Kc encrypted by the distribution key Kd"

multiply encrypting the encrypted first key by a third key;

[see ¶0064 "re-encrypts the contents key Kc by the save key Ks"

encrypting the third key by a predetermined fourth key;

[see ¶0065] the key management center 30 may send these data after encrypting them using the session key established by mutual authentication]

Reference 1 does not explicitly teach:

recording in a recording medium content data encrypted by the first key, the first key encrypted by the predetermined plural types of second keys, and the first key obtained by multiply encrypting the encrypted first key by the second and third keys, and recording the third key encrypted by the fourth key in a security region of the recording medium.

Reference 2 teaches:

see ¶0004, wherein reference 2 teaches of a "tamper resistant memory". It would have been obvious at the time of the invention to one of ordinary skill in the art to which the subject matter pertains to modify the invention taught by reference 1 to record the encryption keys in a security region of the recording medium as disclosed by reference 2 as a "tamper resistant memory. One would be motivated to do this so that the data stored in the tamper resistant memory cannot be easily read out by a third party.

As per claim 2:

A content management method according to claim 1, wherein the first key is provided in plurality, the content data is provided in plurality, each of which is encrypted separately, and the encrypted first key is generated in plurality.

[see reference 1, ¶0066]

As per claim 3:

A content management method according to claim 1, wherein the third key is provided in plurality according to the number of the plurality of first keys provided according to the number of the plurality of content data, and the plurality of encrypted first keys are recorded to be multiply encrypted individually by a plurality of third keys.

[see reference 1, ¶0108]

Art Unit: 2136

As per claim 4:

A content management method according to claim 1, wherein a recording medium having recorded therein the encrypted content data, the first key encrypted by the second key, and the first key multiply encoded by the second and third keys is identical to a recording medium in which there exists a security region in which the third key encrypted by the fourth key is recorded.

[see reference 1, fig. 3 element 100]

As per claim 5:

A content management method according to claim 1, wherein one of the second keys is specific information of the recording medium.

[see reference 1, fig. 3, distribution key Kd]

As per claim 6:

A content management method according to claim 1, wherein the content management method is implemented in a recording apparatus having an encoder module and a drive communicated therewith via an authentication process, and the third key is a key generated only in the drive.

[see reference 1, ¶0065-0066]

As per claim 7:

A content management method according to claim 1, wherein the first key encrypted by the second key and the first key multiply encoded by the second and third keys are recorded in a different recording area of the recording medium.

[see rejection of claim 1, wherein the different recording area of the recording medium is taught by reference 2, "tamper resistant memory".]

As per claim 8:

A content management method according to claim 1, wherein, in the case where content data is moved from the first recording medium to a second recording medium, the content data is re-encrypted after

Art Unit: 2136

being decrypted, the encrypted content data and only the encryption key for controlling movement of content are recorded in the second recording medium, and an encryption key for control movement of contents recorded in the first recording medium is deleted.

[see reference 1, ¶0099, wherein the distribution key is saved to the storage module, and is updated every predetermined period and change from time to time in view of its safety.]

As per claim 9:

A content management method according to claim 8, wherein, in the case where content data is moved to a third recording medium from the second recording medium having recorded therein only the encryption key for controlling movement of contents, the content data is re-encrypted after being decrypted, the encrypted content data and the encryption key for controlling movement of contents are recorded in the third recording medium, and the encryption key for controlling movement of contents of the second recording medium is deleted, thereby carrying out processing for moving contents between the recording mediums.

[see ¶0099 and ¶0101]

As per claim 10:

A content management method according to claim 1, further comprising:
generating key source data by a specific random number generator;

[see reference 1, ¶0075]

multiplying a specific function based on information for specifying the plurality of content data to generate a plurality of third keys;

[see rejection of claim 3]

recording the plurality of third keys as the multiply encrypted key of a plurality of encrypted first keys, with a plurality of encrypted content data and a multiply encrypted first key in a recording medium; and

[see rejection of claim 2]

encrypting the key source data generated by the random number generator by means of a predetermined encryption key, and then, recording the encrypted data in a security region of the recording medium.

[see reference 1, ¶0075, and reference 2, "tamper resistant memory"]

As per claim 13:

A content management method according to claim 1, further comprising:

in a reproduction process of the first recording medium and a second recording medium having recorded therein a security region the encrypted content data, the first key multiply encoded by the second and third keys, and the third key encrypted by the fourth key,

[see reference 1, ¶0064]

in the first recording medium, reading out the first key encrypted by the second key, decrypting the first key encrypted by predetermined plural types of second keys, reading out the encrypted content data, and decrypting content data by the decrypted first key, thereby carrying out reproduction, and

[see reference 1, ¶0064]

in the second recording medium, reading out the third key encrypted from the security region, decrypting the third key encrypted by predetermined plural types of fourth keys, reading out the second key multiply encoded by the second and third keys to detect the first key decrypted by the third key and encrypted by the second key, decrypting the first key encrypted by the predetermined plural types of second keys, and decrypting the encrypted content data by the decrypted first key, thereby carrying out reproduction.

[see reference 1, ¶0066]

As per claim 15:

A recording apparatus according to claim 14, further comprising: processing portions which, in the case where content data is moved from the first recording medium to a second recording medium, encrypts the content data after being decrypted, records only an encrypted content data and an encryption key for controlling movement of contents in the second recording medium, and deletes the encryption key for controlling movement of contents recorded in the first recording medium, and; in the case where content data is moved to a third recording medium from a recording medium having recorded therein only the encryption key for controlling movement of contents as in the second recording medium, re-encrypts content data after being decrypted, recording the encrypted content data and the encryption key for

Art Unit: 2136

controlling movement of contents in the third recording medium, and deletes the encryption key for controlling movement of contents of the second recording medium which is a source medium, thereby carrying out processing for moving content data between the recording mediums.

[see rejections of claims 8 and 9]

As per claim 19:

A recording medium according to claim 18, further comprising, second and third recording mediums which is different from the first recording medium and have recorded therein the content data encrypted by the first key and the encryption key for controlling movement of contents obtained by multiply encrypting the first key.

[see reference 1, fig. 5, element 10, 170, and 180]

Claims 11-12, 16-17, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over reference 1 and reference 2 as applied to claim 1 above, and further in view of Boneh et al., US Patent No. 6,134,660, hereinafter Boneh.

As per claims 11, 16, 17, 20:

A content management method according to claim 1, further comprising: in the case where the first key encrypted by the second key and the first key multiply encoded by the second and third keys each are recorded as independent file data in an independent recording area, providing an encrypted encryption key file having identification information indicating whether file key data is the first key encrypted by the second key or the first key multiply encoded by the second and third keys at the beginning of the key file of the storage area or at a predetermined position and identification information indicating whether a respective counterpart key file exists or not.

Reference 1 and reference 2 have been discussed above. Neither said references explicitly teach of an encrypted key file.

Boneh teaches:

Art Unit: 2136

[see col. 3, ¶3-4, wherein Boneh teaches an encrypted key file. It would have been obvious at the time of the invention to one of ordinary skill in the art to which the subject matter pertains to modify the teachings of references 1 and 2 to include the usage of an encrypted key file. One would be motivated to do this in order to backup and store records of key usage in order to protect against accidental file erasure or system crashes.

As per claim 12:

A content management method according to claim 11, wherein the encrypted encryption key file is multiply written a plurality of times.

[see Boneh, ¶3]

CONCLUSION

The art made of record and not relied upon is considered pertinent to applicant's disclosure.

POINTS OF CONTACT

- * Any response to this Office Action should be **faxed to (571) 273-8300 or mailed to:**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

- * Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Daniel L. Hoang
4/06/07

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


4,6107